

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-265317

(43)Date of publication of application : 28.09.1999

(51)Int.Cl. G06F 12/14
G06F 12/14
G06F 12/00
G06F 17/00
G09C 1/00
G09C 1/00
H04L 9/08

(21)Application number : 10-065766

(71)Applicant : NIPPON TELEGR & TELEPH
CORP <NTT>

(22)Date of filing : 16.03.1998

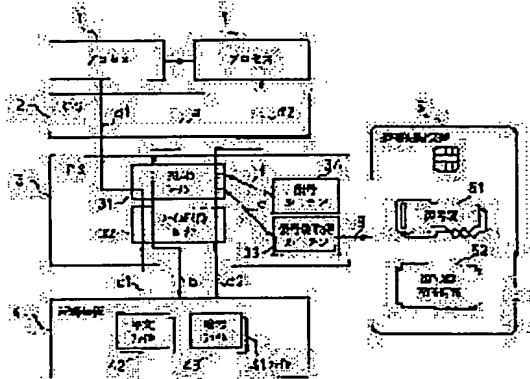
(72)Inventor : TAKEI HIDEAKI
MORIYASU KENJI

(54) COPYRIGHT PROTECTION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a copyright protection system capable of preventing the illegal use of digital data, protecting author's copyright, protecting the copyright of all writers related to the preparation of digital data and providing the application right of the digital data not only in each computer but also in each user.

SOLUTION: When a file of which contents are requested to be read out as reading service is a ciphered file 43, a file system(FS) 3 deciphers data by using a decipher key 51 selected from a portable recorder 5 by using deciphering algorithm expressed by the value of a cipher attribute and the identifier (ID) of the file and transfers the deciphered data to a request source. When the file to be read out is not a ciphered file, the data of the file are transferred to the request source as they are.



【特許請求の範囲】

【請求項 1】 ファイルシステム、オペレーティングシステム、携帯記録装置および鍵管理センタを有する著作権保護システムであって、

前記ファイルシステムは、ファイルの集合を管理し、前記ファイルに関して内容の読み出しサービスを行い、前記ファイルは、記録されるデータ自身に加え、前記データの内容を一意に識別する識別子および属性を有し、前記属性は、前記データが暗号化されている場合は対応する復号アルゴリズムを示す値を持ち、前記データが暗号化されていない場合は暗号化されていないことを示す値を持つ暗号属性を有し、

前記オペレーティングシステムは、アプリケーションプロセスを管理し、該アプリケーションプロセスから前記ファイルシステムへの前記ファイル内容の読み出し操作を含む前記アプリケーションプロセスに関わる全入出力処理を制御し、

前記携帯記録装置は、ユーザによる携帯が可能であり、ユーザが本システムを利用する時だけ、本システムに接続され、前記識別子に対応する復号鍵が格納され、前記鍵管理センタは、前記識別子と前記復号鍵を対にして管理し、

前記ファイルシステムは、前記ファイル内容の読み出しサービスを要求された場合については、対象となる前記ファイルが前記暗号属性に復号アルゴリズムを示す値が設定されている暗号ファイルであるとき、前記暗号属性の値が意味する復号アルゴリズムと前記ファイルの前記識別子を使って前記携帯記録装置から選択した前記復号鍵を用いて前記データを復号し、取得した復号データを要求元に渡し、対象となる前記ファイルが前記暗号ファイルでないとき、前記ファイルの前記データをそのまま要求元に渡し、

前記オペレーティングシステムは、前記アプリケーションプロセスに対し、前記ファイルシステムから前記ファイル内容の読み出しサービスを使って前記暗号ファイルから読み出したデータを渡す場合、前記アプリケーションプロセスによる前記アプリケーションプロセス以外への前記データの引き渡しに制限を与えることを特徴とする著作権保護システム。

【請求項 2】 ファイルシステムおよびオペレーティングシステムを有する著作権保護システムであって、前記ファイルシステムは、ファイルの集合を管理し、前記ファイルに関してコピー読み出しサービスを行い、前記ファイルは、記録されるデータ自身に加え、前記データの内容を一意に識別する識別子および属性を有し、前記属性は、前記データが暗号化されている場合は対応する復号アルゴリズムを示す値を持ち、前記データが暗号化されていない場合は暗号化されていないことを示す値を持つ暗号属性を有し、前記オペレーティングシステムは、アプリケーションプ

ロセスを管理し、該アプリケーションプロセスから前記ファイルシステムへの前記ファイルのコピー読み出し操作を含む前記アプリケーションプロセスに関わる全入出力処理を制御し、

前記ファイルシステムは、前記ファイルのコピー読み出しサービスを要求された場合については、対象となる前記ファイルの前記暗号属性の値に関わらず前記ファイルの前記データをそのまま要求元に渡すことを特徴とする著作権保護システム。

10 【請求項 3】 ファイルシステムおよびオペレーティングシステムを有する著作権保護システムであって、前記ファイルシステムは、ファイルの集合を管理し、前記ファイルに関して書き込みサービスを行い、前記ファイルは、記録されるデータ自身に加え、前記データの内容を一意に識別する識別子および属性を有し、前記属性は、前記データが暗号化されている場合は対応する復号アルゴリズムを示す値を持ち、前記データが暗号化されていない場合は暗号化されていないことを示す値を持つ暗号属性を有し、

20 前記オペレーティングシステムは、アプリケーションプロセスを管理し、該アプリケーションプロセスから前記ファイルシステムへの前記ファイルの書き込み操作を含む前記アプリケーションプロセスに関わる全入出力処理を制御し、

前記ファイルシステムは、前記ファイルの書き込みサービスを要求された場合については、該要求と共に渡されたデータを同じく要求と共に渡された前記識別子および前記暗号属性を属性として持つ前記ファイルとして書き込むことを特徴とする著作権保護システム。

30 【請求項 4】 ファイルシステム、オペレーティングシステム、携帯記録装置、および鍵管理センタを有する著作権保護システムであって、

前記ファイルシステムは、ファイルの集合を管理し、前記ファイルに関して内容の読み出し、コピー読み出し、および書き込みサービスを行い、

前記ファイルは、記録されるデータ自身に加え、前記データの内容を世界的に一意に識別する識別子およびいくつかの属性を有し、

40 前記属性は、前記データが暗号化されている場合は対応する復号アルゴリズムを示す値を持ち、前記データが暗号化されていない場合は暗号化されていないことを示す値を持つ暗号属性を有し、

前記オペレーティングシステムは、アプリケーションプロセスを管理し、該アプリケーションプロセスから前記ファイルシステムへの前記ファイル内容の読み出し、ファイルコピー読み出し、ファイル書き込みの操作を含む前記アプリケーションプロセスに関わる全入出力処理を制御し、

50 前記携帯記録装置は、ユーザによる携帯が可能であり、ユーザが本システムを利用する時だけ、本システムに接

続され、前記識別子に対応する復号鍵が格納され、前記鍵管理センタは、前記識別子と前記復号鍵を対にして管理し、前記ファイルシステムは、前記ファイル内容の読み出しサービスを要求された場合については、対象となる前記ファイルが前記暗号属性に復号アルゴリズムを示す値が設定されている暗号ファイルであるとき、前記暗号属性の値が意味する復号アルゴリズムと前記ファイルの前記識別子を使って前記携帯記録装置から選択した前記復号鍵を用いて前記データを復号し、取得した復号データを要求元に渡し、対象となる前記ファイルが前記暗号ファイルでないとき、前記ファイルの前記データをそのまま要求元に渡し、前記ファイルのコピー読み出しサービスを要求された場合については、対象となる前記ファイルの前記暗号属性の値に関わらず前記ファイルの前記データをそのまま要求元に渡し、前記ファイルの書き込みサービスを要求された場合については、要求と共に渡されたデータを同じく要求と共に渡された前記識別子および前記暗号属性を属性として持つ前記ファイルとして書き込み、前記オペレーティングシステムは、前記アプリケーションプロセスに対し、前記ファイルシステムから前記内容読み出しサービスを使って前記暗号ファイルから読み出したデータを渡す場合、前記アプリケーションプロセスによる前記アプリケーションプロセス以外への前記データの引き渡しに制限を与えることを特徴とする著作権保護システム。

【請求項 5】 前記ファイルシステムは、前記暗号ファイルを対象とした前記ファイル内容の読み出しサービスを要求された場合に、前記識別子に対応する適切な前記復号鍵を前記携帯記録装置から選択できなかったとき、要求元に読み出しエラーを返すことを特徴とする請求項 1 または 4 記載の著作権保護システム。

【請求項 6】 前記データの著作者が前記データを暗号化した暗号データを、前記データの内容を一意に示す前記識別子および前記暗号データを復号化するための復号アルゴリズムを示す前記暗号属性を属性として有する前記ファイルとして書き込むことを特徴とする請求項 3 または 4 記載の著作権保護システム。

【請求項 7】 前記暗号データを含む前記ファイルは、前記ファイルのコピー読み出しおよびファイルの書き込みサービスの組み合わせで自由にコピー可能であり、ユーザが利用するためには前記暗号データを復号する前記復号鍵が必要であり、著作者はユーザに前記復号鍵を供給可能とするために、前記ファイルに関する前記識別子および前記復号鍵の組を前記鍵管理センタへ登録することを特徴とする請求項 4 記載の著作権保護システム。

【請求項 8】 前記暗号データを含む前記ファイルの利用を希望するユーザは、前記鍵管理センタに対し前記ファイルの前記識別子に対応する前記復号鍵の取得を要求

し、前記鍵管理センタは要求したユーザに対し代価の支払等を確認した後、要求された前記復号鍵を前記識別子と共に要求したユーザの前記携帯記録装置に記録することを特徴とする請求項 1 または 4 記載の著作権保護システム。

【請求項 9】 前記属性は、零個または複数のリンク属性を有し、前記リンク属性は、リンク先ファイル名、挿入位置、挿入部位および読み出しエラー対処を含む項目を有し、前記ファイルは、前記リンク属性を少なくとも 1 つ持つとき、リンク元ファイルとなり、前記ファイルシステムは、前記リンク属性のない前記ファイルを対象とした前記ファイル内容の読み出しサービスを要求された場合、対象となった前記ファイルに対して前記ファイル内容の読み出し動作を実行し、前記ファイルシステムは、前記リンク属性を持つ前記ファイルを対象とした前記ファイル内容の読み出しサービスを要求された場合、まず 1 つの前記リンク属性について前記リンク先ファイル名に示される前記ファイルを対象とした前記ファイル内容の読み出しサービスを自らに再帰的に要求することによって読み出し結果を取得し、読み出しに成功したときは、取得したデータから前記挿入部位に示される部分を抽出して得たデータを前記リンク元ファイルの前記データ中における指定の位置である前記挿入位置に示される位置に挿入し、読み出しに失敗したときは、前記読み出しエラー対処に示される処理を実行し、次の残りの前記リンク属性について上記操作を繰り返し実行し、前記リンク元ファイルにおけるすべてのリンク属性に対して上記操作が終了した後、挿入の終わった前記リンク元ファイルの前記データを要求元に渡すことを特徴とする請求項 1 または 4 記載の著作権保護システム。

【請求項 10】 前記リンク属性は、更に非展開対処の項目を有し、前記ファイルシステムは、前記ファイル内容の読み出しサービスのモードとして非展開モードを提供し、前記ファイルシステムは、前記リンク元ファイルを対象とした前記ファイル内容の読み出しサービスを前記非展開モードで要求された場合、すべてのリンク属性に対してそれぞれの非展開対処に示される処理を実行することを特徴とする請求項 9 記載の著作権保護システム。

【請求項 11】 前記属性は、暗号属性と零個または複数のリンク属性を有し、前記ファイルシステムは、前記リンク元ファイルを対象とした前記ファイル内容の読み出しサービスを要求されたとき、前記暗号属性に基づいた復号を実行した後、前記リンク属性に基づく挿入を行い、前記オペレーティングシステムは、前記アプリケーションプロセスに前記ファイル内容の読み出しの結果として前記リンク元ファイルの前記データを渡す場合で、一連

の前記ファイル内容の読み出しの対象となった前記ファイルのうち少なくとも1つの前記暗号属性に復号アルゴリズムを示す値が設定されているとき、前記アプリケーションプロセスによる前記アプリケーションプロセス以外への情報提供に制限を与えることを特徴とする請求項9記載の著作権保護システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ユーザ間におけるデータのコピー等によるデータ流通は許容しつつも、そのデータを利用するには別途各ユーザが利用権を取得する必要を生じせしめ、またデータ甲の全部あるいは一部分を内部に含むデータ乙をユーザが利用する際に、データ乙におけるデータ甲の部分を利用するには別途各ユーザがデータ甲に対する利用権を取得する必要を生じせしめることで、データの著作権者の権利を保護できる著作権保護システムに関する。

【0002】

【従来の技術】コンピュータにおけるデジタルデータの単位としてはファイルが使用されている。ファイルは、ネットワーク等を用いてコンピュータ間で容易に、誤りなく、しかも高速にコピー可能であり、デジタルデータの大きな特徴となっている。

【0003】一般的なコンピュータシステムにおけるファイルの読み出し手順について図10を参照して説明する。このコンピュータシステムは、プロセス101、オペレーティングシステム（以下、OSと略称する）102、ファイルシステム（以下、FSと略称する）103、複数のファイル141を格納する記録装置104から構成されている。

【0004】プロセス101が記録装置104からファイル141を読み出す動作では、プロセス101は、OS102を通じてFS103に対して1つのファイル141の読み出しを要求する（a）。要求を受けたFS103は記録装置104へ該ファイル141の読み出しを要求して（b）、読み出し結果を取得し（c）、この取得した読み出し結果をOS102を通じてプロセス101に返送する（d）。

【0005】このようにデジタルデータの単位としてファイルを使用するシステムにおいては、例えばあるユーザが正当に取得し利用しているファイルを別のユーザがコピーすることによって不正に取得し利用することも容易にし、著作物としてのファイルと考えたとき、ファイルの著作権者の著作権を保護することに対する大きな障害となる。

【0006】アプリケーション固有の非公開なファイルフォーマットによって、扱うファイルの著作権を保護する方法があるが、これは汎用的なファイルフォーマットには適用できない。デジタルデータのもう1つの特徴に、カット・アンド・ペーストに象徴されるような、他

のデータの引用、流用等の再利用が容易であるという点がある。

【0007】このように他のデータを再利用して作成されたデータにおいては、利用された他のデータの作成者を含む作成に関与したすべての作成者に対して著作権を保護すべきであるが、従来のカット・アンド・ペーストではデータのコピーしか行わないので、これらの著作権は保護することに対する障害となる。

【0008】著作権保護のためにデジタルデータのコンピュータへのインストールに制限を課す方法があるが、この制限により正当な権利を持つユーザであっても、別のコンピュータでは利用できなかったり、あるいは正当な権利を持たないユーザが利用することもできてしまう。

【0009】

【発明が解決しようとする課題】上述したように、従来の方法ではファイルの不正取得が容易であるため、著作物としてのファイルと考えたとき、ファイルの著作権者の著作権を保護することに対する大きな障害となっている。

【0010】また、例えばカット・アンド・ペースト等を利用して、他のデータの引用、流用等の再利用により作成したデータに対しては、利用された他のデータの作成者を含む作成に関与したすべての作成者に対する著作権の保護を完全に行うことができない。

【0011】更に、著作権保護のためにコンピュータへのインストールに制限を課す従来の方法では、正当な権利を持つユーザも別のコンピュータでは利用できなかったり、または正当な権利を持たないユーザも利用することができてしまうという問題がある。

【0012】本発明は、上記に鑑みてなされたもので、その目的とするところは、デジタルデータの不正利用を防止し、著作権者の著作権を保護し、デジタルデータの作成に関与したすべての作成者に対する著作権を保護し、デジタルデータに対する利用権をコンピュータ毎でなくユーザ毎にも付与可能にする著作権保護システムを提供することにある。

【0013】

【課題を解決するための手段】上記目的を達成するため、請求項1記載の本発明は、ファイルシステム、オペレーティングシステム、携帯記録装置および鍵管理センタを有する著作権保護システムであって、前記ファイルシステムは、ファイルの集合を管理し、前記ファイルに関して内容の読み出しサービスを行い、前記ファイルは、記録されるデータ自身に加え、前記データの内容を一意に識別する識別子および属性を有し、前記属性は、前記データが暗号化されている場合は対応する復号アルゴリズムを示す値を持ち、前記データが暗号化されていない場合は暗号化されていないことを示す値を持つ暗号属性を有し、前記オペレーティングシステムは、アプリ

ケーションプロセスを管理し、該アプリケーションプロセスから前記ファイルシステムへの前記ファイル内容の読み出し操作を含む前記アプリケーションプロセスに関わる全入出力処理を制御し、前記携帯記録装置は、ユーザによる携帯が可能であり、ユーザが本システムを利用する時だけ、本システムに接続され、前記識別子に対応する復号鍵が格納され、前記鍵管理センタは、前記識別子と前記復号鍵を対にして管理し、前記ファイルシステムは、前記ファイル内容の読み出しサービスを要求された場合については、対象となる前記ファイルが前記暗号属性に復号アルゴリズムを示す値が設定されている暗号ファイルであるとき、前記暗号属性の値が意味する復号アルゴリズムと前記ファイルの前記識別子を使って前記携帯記録装置から選択した前記復号鍵を用いて前記データを復号し、取得した復号データを要求元に渡し、対象となる前記ファイルが前記暗号ファイルでないとき、前記ファイルの前記データをそのまま要求元に渡し、前記オペレーティングシステムは、前記アプリケーションプロセスに対し、前記ファイルシステムから前記ファイル内容の読み出しサービスを使って前記暗号ファイルから読み出したデータを渡す場合、前記アプリケーションプロセスによる前記アプリケーションプロセス以外への前記データの引き渡しに制限を与えることを要旨とする。

【0014】請求項1記載の本発明にあっては、ファイルシステムはファイル内容の読み出しサービスを要求された場合については、対象となるファイルが暗号ファイルであるとき、暗号属性の値が意味する復号アルゴリズムとファイルの識別子を使って携帯記録装置から選択した復号鍵を用いてデータを復号し、復号データを要求元に渡し、対象となるファイルが暗号ファイルでないとき、ファイルのデータをそのまま要求元に渡し、オペレーティングシステムはアプリケーションプロセスに対し、ファイルシステムからファイル内容の読み出しサービスを使って暗号ファイルから読み出したデータを渡す場合、アプリケーションプロセスによるアプリケーションプロセス以外へのデータの引き渡しに制限を与えている。

【0015】また、請求項2記載の本発明は、ファイルシステムおよびオペレーティングシステムを有する著作権保護システムであって、前記ファイルシステムは、ファイルの集合を管理し、前記ファイルに関してコピー読み出しサービスを行い、前記ファイルは、記録されるデータ自身に加え、前記データの内容を一意に識別する識別子および属性を有し、前記属性は、前記データが暗号化されている場合は対応する復号アルゴリズムを示す値を持ち、前記データが暗号化されていない場合は暗号化されていないことを示す値を持つ暗号属性を有し、前記オペレーティングシステムは、アプリケーションプロセスを管理し、該アプリケーションプロセスから前記ファイルシステムへの前記ファイルのコピー読み出し操作を

含む前記アプリケーションプロセスに関わる全入出力処理を制御し、前記ファイルシステムは、前記ファイルのコピー読み出しサービスを要求された場合については、対象となる前記ファイルの前記暗号属性の値に関わらず前記ファイルの前記データをそのまま要求元に渡すことを要旨とする。

【0016】請求項2記載の本発明にあっては、オペレーティングシステムは、アプリケーションプロセスを管理し、該アプリケーションプロセスからファイルシステムへのファイルのコピー読み出し操作を含むアプリケーションプロセスに関わる全入出力処理を制御し、ファイルシステムは、ファイルのコピー読み出しサービスを要求された場合については、対象となるファイルの暗号属性の値に関わらずファイルのデータをそのまま要求元に渡している。

【0017】更に、請求項3記載の本発明は、ファイルシステムおよびオペレーティングシステムを有する著作権保護システムであって、前記ファイルシステムは、ファイルの集合を管理し、前記ファイルに関して書き込みサービスを行い、前記ファイルは、記録されるデータ自身に加え、前記データの内容を一意に識別する識別子および属性を有し、前記属性は、前記データが暗号化されている場合は対応する復号アルゴリズムを示す値を持ち、前記データが暗号化されていない場合は暗号化されていないことを示す値を持つ暗号属性を有し、前記オペレーティングシステムは、アプリケーションプロセスを管理し、該アプリケーションプロセスから前記ファイルシステムへの前記ファイルの書き込み操作を含む前記アプリケーションプロセスに関わる全入出力処理を制御し、前記ファイルシステムは、前記ファイルの書き込みサービスを要求された場合については、該要求と共に渡されたデータを同じく要求と共に渡された前記識別子および前記暗号属性を属性として持つ前記ファイルとして書き込むことを要旨とする。

【0018】請求項3記載の本発明にあっては、オペレーティングシステムは、アプリケーションプロセスを管理し、該アプリケーションプロセスからファイルシステムへのファイルの書き込み操作を含むアプリケーションプロセスに関わる全入出力処理を制御し、ファイルシステムは、ファイルの書き込みサービスを要求された場合については、該要求と共に渡されたデータを同じく要求と共に渡された識別子および暗号属性を属性として持つファイルとして書き込む。

【0019】また、請求項4記載の本発明は、ファイルシステム、オペレーティングシステム、携帯記録装置、および鍵管理センタを有する著作権保護システムであって、前記ファイルシステムは、ファイルの集合を管理し、前記ファイルに関して内容の読み出し、コピー読み出し、および書き込みサービスを行い、前記ファイルは、記録されるデータ自身に加え、前記データの内容を

世界的に一意に識別する識別子およびいくつかの属性を有し、前記属性は、前記データが暗号化されている場合は対応する復号アルゴリズムを示す値を持ち、前記データが暗号化されていない場合は暗号化されていないことを示す値を持つ暗号属性を有し、前記オペレーティングシステムは、アプリケーションプロセスを管理し、該アプリケーションプロセスから前記ファイルシステムへの前記ファイル内容の読み出し、ファイルコピー読み出し、ファイル書き込みの操作を含む前記アプリケーションプロセスに関わる全入出力処理を制御し、前記携帯記録装置は、ユーザによる携帯が可能であり、ユーザが本システムを利用する時だけ、本システムに接続され、前記識別子に対応する復号鍵が格納され、前記鍵管理センタは、前記識別子と前記復号鍵を対にして管理し、前記ファイルシステムは、前記ファイル内容の読み出しサービスを要求された場合については、対象となる前記ファイルが前記暗号属性に復号アルゴリズムを示す値が設定されている暗号ファイルであるとき、前記暗号属性の値が意味する復号アルゴリズムと前記ファイルの前記識別子を使って前記携帯記録装置から選択した前記復号鍵を用いて前記データを復号し、取得した復号データを要求元に渡し、対象となる前記ファイルが前記暗号ファイルでないとき、前記ファイルの前記データをそのまま要求元に渡し、前記ファイルのコピー読み出しサービスを要求された場合については、対象となる前記ファイルの前記暗号属性の値に関わらず前記ファイルの前記データをそのまま要求元に渡し、前記ファイルの書き込みサービスを要求された場合については、要求と共に渡されたデータを同じく要求と共に渡された前記識別子および前記暗号属性を属性として持つ前記ファイルとして書き込み、前記オペレーティングシステムは、前記アプリケーションプロセスに対し、前記ファイルシステムから前記内容読み出しサービスを使って前記暗号ファイルから読み出したデータを渡す場合、前記アプリケーションプロセスによる前記アプリケーションプロセス以外への前記データの引き渡しに制限を与えることを要旨とする。

【0020】請求項4記載の本発明にあつては、ファイルシステムはファイル内容の読み出しサービスを要求された場合については、対象ファイルが暗号ファイルであるとき、暗号属性の値が意味する復号アルゴリズムとファイルの識別子を使って携帯記録装置から選択した復号鍵を用いてデータを復号して、復号データを要求元に渡し、対象ファイルが暗号ファイルでないとき、ファイルのデータをそのまま要求元に渡し、ファイルのコピー読み出しサービスを要求された場合については、対象ファイルの暗号属性の値に関わらずファイルのデータをそのまま要求元に渡し、ファイルの書き込みサービスを要求された場合については、該要求と共に渡されたデータを同じく要求と共に渡された識別子および暗号属性を属性として持つファイルとして書き込み、オペレーティング

システムはアプリケーションプロセスに対してファイルシステムから内容読み出しサービスを使って暗号ファイルから読み出したデータを渡す場合、アプリケーションプロセスによるアプリケーションプロセス以外へのデータの引き渡しに制限を与えている。

【0021】更に、請求項5記載の本発明は、請求項1または4記載の発明において、前記ファイルシステムが、前記暗号ファイルを対象とした前記ファイル内容の読み出しサービスを要求された場合に、前記識別子に対応する適切な前記復号鍵を前記携帯記録装置から選択できなかったとき、要求元に読み出しエラーを返すことを要旨とする。

【0022】請求項5記載の本発明にあつては、ファイルシステムは暗号ファイルを対象としたファイル内容の読み出しサービスを要求された場合に、識別子に対応する適切な復号鍵を携帯記録装置から選択できなかったとき、要求元に読み出しエラーを返す。

【0023】請求項6記載の本発明は、請求項3または4記載の発明において、前記データの著作者が前記データを暗号化した暗号データを、前記データの内容を一意に示す前記識別子および前記暗号データを復号化するための復号アルゴリズムを示す前記暗号属性を属性として有する前記ファイルとして書き込むことを要旨とする。

【0024】請求項6記載の本発明にあつては、データの内容を一意に示す識別子および復号アルゴリズムを示す暗号属性を属性として有するファイルとして暗号データを書き込む。

【0025】また、請求項7記載の本発明は、請求項4記載の発明において、前記暗号データを含む前記ファイルが、前記ファイルのコピー読み出しおよびファイルの書き込みサービスの組み合わせで自由にコピー可能であり、ユーザが利用するためには前記暗号データを復号する前記復号鍵が必要であり、著作者はユーザに前記復号鍵を供給可能とするために、前記ファイルに関する前記識別子および前記復号鍵の組を前記鍵管理センタへ登録することを要旨とする。

【0026】請求項7記載の本発明にあつては、暗号データを含むファイルはファイルのコピー読み出しおよびファイルの書き込みサービスの組み合わせで自由にコピー可能であり、ユーザが利用するためには暗号データを復号する復号鍵が必要であり、著作者はユーザに復号鍵を供給可能とするためにファイルに関する識別子および復号鍵の組を鍵管理センタへ登録する。

【0027】更に、請求項8記載の本発明は、請求項1または4記載の発明において、前記暗号データを含む前記ファイルの利用を希望するユーザが、前記鍵管理センタに対し前記ファイルの前記識別子に対応する前記復号鍵の取得を要求し、前記鍵管理センタは要求したユーザに対し代価の支払等を確認した後、要求された前記復号鍵を前記識別子と共に要求したユーザの前記携帯記録装

置に記録することを要旨とする。

【0028】請求項8記載の本発明にあっては、ユーザは鍵管理センタに復号鍵の取得を要求し、鍵管理センタはユーザに対し代価の支払等を確認した後、復号鍵を識別子と共にユーザの携帯記録装置に記録する。

【0029】請求項9記載の本発明は、請求項1または4記載の発明において、前記属性は、零個または複数個のリンク属性を有し、前記リンク属性は、リンク先ファイル名、挿入位置、挿入部位および読み出しエラー対処を含む項目を有し、前記ファイルは、前記リンク属性を少なくとも1つ持つとき、リンク元ファイルとなり、前記ファイルシステムは、前記リンク属性のない前記ファイルを対象とした前記ファイル内容の読み出しサービスを要求された場合、対象となった前記ファイルに対して前記ファイル内容の読み出し動作を実行し、前記ファイルシステムは、前記リンク属性を持つ前記ファイルを対象とした前記ファイル内容の読み出しサービスを要求された場合、まず1つの前記リンク属性について前記リンク先ファイル名に示される前記ファイルを対象とした前記ファイル内容の読み出しサービスを自らに再帰的に要求することによって読み出し結果を取得し、読み出しに成功したときは、取得したデータから前記挿入部位に示される部分を抽出して得たデータを前記リンク元ファイルの前記データ中における指定の位置である前記挿入位置に示される位置に挿入し、読み出しに失敗したときは、前記読み出しエラー対処に示される処理を実行し、次の残りの前記リンク属性について上記操作を繰り返し実行し、前記リンク元ファイルにおけるすべてのリンク属性に対して上記操作が終了した後、挿入の終わった前記リンク元ファイルの前記データを要求元に渡すことを要旨とする。

【0030】請求項9記載の本発明にあっては、ファイルシステムはリンク属性を持つファイルを対象としたファイル内容の読み出しサービスを要求された場合、まず1つのリンク属性についてリンク先ファイル名に示されるファイルを対象としたファイル内容の読み出しサービスを自らに再帰的に要求することによって読み出し結果を取得し、読み出しに成功したときは、取得データから挿入部位に示される部分を抽出して得たデータをリンク元ファイルのデータ中の挿入位置に挿入し、読み出しに失敗したときは、読み出しエラー対処に示される処理を実行し、次に残りのリンク属性について上記操作を繰り返し実行し、リンク元ファイルにおけるすべてのリンク属性に対して上記操作が終了した後、挿入の終わったリンク元ファイルのデータを要求元に渡す。

【0031】また、請求項10記載の本発明は、請求項9記載の発明において、前記リンク属性は、更に非展開対処の項目を有し、前記ファイルシステムは、前記ファイル内容の読み出しサービスのモードとして非展開モードを提供し、前記ファイルシステムは、前記リンク元フ

ァイルを対象とした前記ファイル内容の読み出しサービスを前記非展開モードで要求された場合、すべてのリンク属性に対してそれぞれの非展開対処に示される処理を実行することを要旨とする。

【0032】請求項10記載の本発明にあっては、ファイルシステムはリンク元ファイルを対象としたファイル内容の読み出しサービスを非展開モードで要求された場合、すべてのリンク属性に対してそれぞれの非展開対処に示される処理を実行する。

【0033】更に、請求項11記載の本発明は、請求項9記載の発明において、前記属性が、暗号属性と零個または複数個のリンク属性を有し、前記ファイルシステムは、前記リンク元ファイルを対象とした前記ファイル内容の読み出しサービスを要求されたとき、前記暗号属性に基づいた復号を実行した後、前記リンク属性に基づく挿入を行い、前記オペレーティングシステムは、前記アプリケーションプロセスに前記ファイル内容の読み出しの結果として前記リンク元ファイルの前記データを渡す場合で、一連の前記ファイル内容の読み出しの対象となった前記ファイルのうち少なくとも1つの前記暗号属性に復号アルゴリズムを示す値が設定されているとき、前記アプリケーションプロセスによる前記アプリケーションプロセス以外への情報提供に制限を与えることを要旨とする。

【0034】請求項11記載の本発明にあっては、ファイルシステムはリンク元ファイルを対象としたファイル内容の読み出しサービスを要求されたとき暗号属性に基づいた復号を実行した後、リンク属性に基づく挿入を行い、オペレーティングシステムはアプリケーションプロセスにファイル内容の読み出しの結果としてリンク元ファイルのデータを渡す場合で、一連のファイル内容の読み出しの対象となったファイルのうち少なくとも1つの暗号属性に復号アルゴリズムを示す値が設定されているとき、アプリケーションプロセスによるアプリケーションプロセス以外への情報提供に制限を与えている。

【0035】

【発明の実施の形態】図面を参照して説明する前に、まず本発明の著作権保護システムの概要について説明する。

【0036】ファイルの著作権者の著作権保護に対しては、著作権者がファイルを暗号化し、正当なユーザのみにそのファイルの復号化に必要な復号鍵を渡す方法が有効である。暗号化されたファイル（以下、暗号ファイルと称する）は復号鍵によって復号されてはじめて意味があり、利用価値のあるものになるのであり、復号鍵を持たないユーザ、つまり正当でないユーザ（以下、不正なユーザと称する）に対しては、まったく利用価値がない。従って、不正なユーザは、暗号ファイルを取得したからといってその暗号ファイルを利用することはできないから、不正なユーザによるファイルの利用を防ぐという著

著作権保護の1つの目的が達成されると同時に、暗号ファイルが不正ユーザに渡っても著作権保護に対する脅威とはならないので、暗号ファイルを自由に流通させることができる。また、復号鍵を渡す過程においてユーザから対価を徴収することができるから、利用権の譲渡に伴ってユーザから確実に代価を徴収するという著作権保護のもう1つの目的も達成される。

【0037】上記の著作権保護方法に対する信頼性は、正当なユーザのみが復号鍵を所持し、不正なユーザはこの復号鍵を所持しないという仮定に基づくものであり、例えば、不正なユーザが、正当なユーザが所持する復号鍵をコピーするなどして、取得できるようなことがあれば、それは上記著作権保護方法に対する脅威となる。本発明による著作権保護システム（以下、本システムと称する）は復号鍵を携帯記録装置に格納する。携帯記録装置は、例えばICカードのような何らかのセキュリティ機構が備わったユーザによって携帯可能な記録装置であり、ユーザにより格納されているデータの取得やコピーが困難なものである。これにより、不正なユーザによる復号鍵の違法コピーを防ぎ、上記の仮定を保証するとともに、暗号ファイルが格納されているコンピュータであればどこでも利用可能となる。

【0038】暗号ファイルの著作者は、ユーザが鍵管理センタから復号鍵を取得可能にするために、その作成した暗号ファイルに対応する復号鍵を鍵管理センタへ登録する。

【0039】このとき、あるファイルに対応する復号鍵を鍵管理センタから選ぶためには、そのファイルと復号鍵に何らかの関係がなければならない。本システムでは、ファイルに、そのファイルの内容を世界的に一意に識別するための識別子を付与可能である。この識別子はファイルの著作者によって付与される。そして、上記の鍵管理センタとのやりとりには識別子が介在する。

【0040】つまり、著作者は世界的に一意な識別子を選び、作成した暗号ファイルに付与し、この識別子と、この暗号ファイルに対応する復号鍵との組を鍵管理センタへ登録する。ユーザは利用を希望するファイルの識別子を抽出し、この識別子をもって鍵管理センタへ復号鍵を要求する。ユーザの識別子による復号鍵の要求にあたって、識別子は世界的に一意であるから、復号鍵として間違っただけものが要求の結果として返されることはない。

【0041】また、携帯記録装置へ復号鍵を格納する際もこの識別子との組によって格納される。上と同様の理由で、識別子を使うことで適切な復号鍵を携帯記録装置の中から取得することが可能である。

【0042】また、本システムにあつては、復号鍵の引き渡し利用権の引き渡しに相当するものであり、鍵管理センタからユーザへ鍵を引き渡す際、ユーザから何らかの代価の支払いを確認した後に、ユーザの携帯記録装置に復号鍵を格納することによって、利用権の譲渡に伴

うユーザからの課金を確実にする。

【0043】本システムにおける上記鍵管理センタからユーザへの復号鍵の引き渡しにあつては、ネットワークを通じてオンラインでこれを行うことも可能である。ネットワークによる情報伝送は利便性に優れるが、盗聴や改竄といったセキュリティ上の問題があり、伝送する情報に対する盗聴や改竄を防ぐためには、通常よりもコストをかけてセキュリティを強化した方法で伝送する必要がある。オンラインによる復号鍵の引き渡しにおいては、復号鍵に対する盗聴や改竄により不正なユーザが復号鍵を取得したり、正当なユーザが正しい復号鍵を取得できない等の問題を発生するため、復号鍵はセキュリティを強化した方法で伝送される必要がある。そしてこれは通常の伝送方法よりも高コストになる。しかし一般的に、復号鍵は対応するファイルに比べてはるかにサイズが小さいものであり、ファイル全体をセキュリティの高い方法で伝送することに比べれば、はるかに少ないコストで済ますことができる。対応する暗号ファイルの方は通常の低コストな方法で伝送してよい。

【0044】本システムでは暗号ファイルの復号化はファイルシステム内で行われる。ファイルシステムによる復号にあつては、対象となる暗号ファイルに付随している情報である暗号属性と識別子を用いる。暗号属性は復号アルゴリズムを示し、識別子は前述の通り暗号ファイルの内容を世界的に一意に識別する。ファイルシステムは識別子を用いて携帯記録装置から適切な復号鍵を取得し、この取得した復号鍵で暗号ファイルを復号する。用いる復号アルゴリズムは暗号属性に示されるものである。

【0045】また、ユーザやアプリケーションやOSはこの復号化の作業を見ることはないから、あたかも通常の暗号化されていないファイルを扱っているかのように暗号ファイルを扱うことができる。

【0046】本システムでは、ファイルはファイルシステムを通じてOSに渡される。暗号ファイルはファイルシステム内で復号化されるからOSは復号化されたファイル（以下、復号ファイルと称する）を取得することになる。そうして、復号ファイルを別のファイルにセーブすることを考えると、この復号ファイルは不正なユーザに対しても意味があり、利用価値のあるファイルであるから、これは著作権保護に対する脅威になる。つまり、OSは復号ファイルを別ファイルとしてセーブしたりしない、つまり復号ファイルを外部へ流出させない、信頼できるものでなければならない。本システムでは、OSは信頼できるものであるとする。

【0047】ファイルは大きく実行形式ファイルとデータファイルの2種類に分類される。実行形式ファイルを実行する時、実行形式ファイルはファイルシステムによって読み出され、OSに渡され、OS内で解釈実行されるから、実行形式ファイルの情報はOS内で閉じてい

る。しかし、データファイルの場合は、典型的には、データファイルの情報はアプリケーションに渡される。例えば、テキストデータは、テキストエディタに渡されて利用される。つまり、データファイルの情報はOS内にとどまらず、アプリケーションに渡される。

【0048】本システムにおいてデータファイルを暗号化して著作権保護することを考えたとき、この暗号化されたファイルはファイルシステム内で復号化され、データファイルの情報はアプリケーションに渡れることから、アプリケーションは復号化されたファイルを取得できることになる。このように復号ファイルを取得したアプリケーションがこの復号ファイルを別ファイルにセーブするなどして復号ファイルの情報を流出させることは、著作権保護に対する脅威となり、問題となる。

【0049】本システムにあつては、OSは、復号ファイルを渡すアプリケーションに対して出力制限する。具体的には、ファイルシステムは、OSから読み出しを要求されたファイルが暗号ファイルであり、これを復号してOSに渡す場合、渡したデータが復号ファイルであることをOSに通知する。OSは、ファイルシステムから渡されたデータが復号ファイルであることを知ると、このデータを渡すアプリケーションプロセスに対して、以後あらゆる装置への出力を禁止する。ここで、アプリケーションは複数のアプリケーションプロセスから構成されている。OSはアプリケーションプロセスに関するすべての入出力処理を制御しているので、この制限によって、復号ファイルを渡したアプリケーションから復号ファイルの情報が流出されることはなく、上記の問題は解決される。

【0050】ただし、アプリケーションにあつては、ファイルからの情報をユーザに提供することがその動作の本質である場合がある。例えば、アプリケーションの1つであるテキストビューワは、テキストデータが記録されたファイルを取得し、そのテキストデータを文字図形の並びに置き換えてユーザに提示することに、その本質がある。上記のOSの制限は、ユーザに対する情報提供をも禁止するため、例えば暗号化されたテキストデータは復号化されテキストビューワに渡されるが、テキストビューワはユーザに文字図形の並びを提示することができない。本システムでは、OSは、復号ファイルを渡したアプリケーションプロセスに対してユーザインタフェース装置への出力は認めるとする。ユーザインタフェース装置とは、ディスプレイやスピーカといったようなユーザとのインタフェースに供される装置である。このOSの機能により、上記の場合であってもテキストビューワはユーザに文字図形の並びを提供することができる。

【0051】デジタルデータは、カット・アンド・ペースト等を使ってデータが再利用される場合が多い。別のファイルのデータを利用して新しくファイルを作成し、流通させ、ユーザがこれを利用する場合において、この

新しいファイルには著作権を保護すべき対象となる著作者が2人いる。新しいファイルの著作者と元のファイルの著作者である。以後、別のファイル、元のファイルを元ファイル、新しいファイルを新ファイルと呼ぶ。

【0052】本システムにおいては、各ファイルは複数個設定可能なリンク属性をもつ。例えば、元ファイルを利用した新ファイルを作成する場合は、新ファイルのデータ内に元ファイルのデータを直接埋め込むのではなく、新ファイルのリンク属性として、元ファイルのファイル名を設定する。そしてファイルシステムは、この新ファイルに対する読み出しを要求された場合、まず新ファイルのデータ（以下、新データと称する）を読み出し、次にリンク属性に示されるファイルである元ファイルのデータ（以下、元データと称する）を読み出し、次に新データの中に元データを挿入し、要求元に渡す。

【0053】更に、各ファイルには、暗号化を施すことも可能であり、これまで説明したように暗号化したファイルに対応する復号鍵を所持していないとそのファイルの内容を読み出すことができない。従って、本システムにおいては、上記のように元ファイルを内在する新ファイルをユーザが利用する場合であっても、予め元ファイルを暗号化して配布しておくことによって、元ファイルの著作権を保護することができる。何故ならば、ファイルシステムは、新ファイルに対する読み出し要求があった場合に、動作の1つとして上記のように元データを読み出して新データに挿入するが、この際にユーザが元ファイルに対する適切な復号鍵を所持していないと、元ファイルの内容を適切に読み出すことができないからである。また、新ファイルを暗号化することによって新ファイルの著作権も保護することができる。このように本システムでは、新ファイルの著作者、および元ファイルの著作者に対してそれぞれ独立に著作権を保護することが可能である。また、これらの復号化や挿入などの動作はファイルシステム内で行われるので、ユーザやアプリケーションやOSは、あたかも通常のファイルを扱っているかのようにリンク属性を持つ暗号ファイルを扱うことができる。

【0054】また、本システムでは、ファイルを他人にコピーするなど、ファイルを流通させる場合のために、暗号ファイルであっても復号化せず、リンク属性をもつファイルであっても挿入は行わずにファイルを読み出すコピー読み出しサービスも提供する。

【0055】次に、図面を用いて本発明の実施の形態について説明する。図1は、本発明の一実施形態に係る著作権保護システムの構成を示すブロック図である。同図に示す著作権保護システムは、プロセス1、OS2、FS3、記録装置4、および例えばICカードのような携帯記録装置5から構成されている。FS3は、FSメインルーチン31、ファイル取得ルーチン32、復号鍵取得ルーチン33および復号ルーチン34から構成され

る。図 1 のシステムにおいて、ファイル 4 1 には、平文ファイル 4 2 と暗号ファイル 4 3 という 2 種類がある。図 1 は、プロセス 1 が平文ファイル 4 2 と暗号ファイル 4 3 に対し内容読み出しをする 2 種類の動作を示している。

【0056】図 2 はファイル 4 1 の構成を示しており、ファイル 4 1 は、内容データ 4 1 1、暗号属性 4 1 2 および識別子 4 1 3 から構成される。内容データ 4 1 1 は、ファイル 4 1 として記録される内容を示すデータであり、暗号属性 4 1 2 は、内容データ 4 1 1 の暗号化手法を示すファイル属性であり、例えばあるファイル 4 1 の暗号属性 4 1 2 が暗号化なしを示す場合、該ファイル 4 1 は平文ファイル 4 2 に分類され、暗号属性 4 1 2 が何らかの暗号化手法を示す場合、該ファイル 4 1 は暗号ファイル 4 3 に分類される。識別子 4 1 3 は、内容データ 4 1 1 を世界的に一意に示すファイル属性である。

【0057】携帯記録装置 5 は複数の復号鍵 5 1 および復号鍵管理情報 5 2 から構成される。復号鍵管理情報 5 2 は、識別子 4 1 3 に対応する復号鍵 5 1 を実際に携帯記録装置 5 から取得するための情報（以下、復号鍵の場所と称する）が記録されている。

【0058】本発明によるシステムと図 10 の従来のシステムとの主な違いは、ファイル 4 1 が平文ファイル 4 2 と暗号ファイル 4 3 に分類されている点、読み出し対象のファイル 4 1 が暗号ファイル 4 3 であった場合に、復号化を含むいくつかの処理が FS 3 の中に追加されている点である。

【0059】次に、以上のように構成される著作権保護システムの動作について説明する。プロセス 1 が記録装置 4 からファイル 4 1 を読み出す動作では、プロセス 1 は OS 2 を通じて FS 3 に対して 1 つのファイル 4 1 の読み出しを要求する (a)。この要求を受けた FS 3 は記録装置 4 へ該ファイル 4 1 の読み出しを要求する

(b)。このファイルの読み出し要求において、読み出し対象ファイル 4 1 が、平文ファイル 4 2 の場合、FS メインルーチン 3 1 は、ファイル取得ルーチン 3 2 を通じ、読み出し結果を取得した (c 1) 後、読み出し結果をそのままプロセス 1 へ渡す (d 1)。

【0060】読み出し対象ファイル 4 1 が、暗号ファイル 4 3 の場合、FS メインルーチン 3 1 は、ファイル取得ルーチン 3 2 を通じ、読み出し結果を取得する (c 2)。ここで、取得した情報は、内容データ 4 1 1、暗号属性 4 1 2 および識別子 4 1 3 である。内容データ 4 1 1 は暗号属性 4 1 2 に示される属性アルゴリズムによって暗号化されている。

【0061】FS メインルーチン 3 1 は、まず、内容データ 4 1 1 の復号に必要な復号鍵 5 1 を取得するため、復号鍵取得ルーチン 3 3 に対し、識別子 4 1 3 を渡す (e)。復号鍵取得ルーチン 3 3 は、この識別子 4 1 3 と携帯記録装置 5 内に記録されている復号鍵管理情報 5

2 の情報から適切な復号鍵 5 1 の場所を求めた後、携帯記録装置 5 から適切な復号鍵 5 1 を取得し (g)、これを FS メインルーチン 3 1 へ渡す (e)。FS メインルーチン 3 1 は、内容データ 4 1 1、暗号属性 4 1 2 および復号鍵 5 1 を復号ルーチン 3 4 へ渡し、復号化を依頼する。復号ルーチン 3 4 は、暗号属性 4 1 2 から適切な復号アルゴリズムを選択し、この復号アルゴリズムと復号鍵 5 1 を使って内容データ 4 1 1 を復号し、復号結果を返す (f)、復号結果を取得した FS メインルーチン 3 1 は、復号結果をプロセス 1 へ渡す (d 2)。

【0062】次に、本発明の第 2 の実施形態について図 3 を参照して説明する。この第 2 の実施形態は、移動やコピーといったファイル操作に用いるためのファイルコピー読み出しに関するものであり、第 1 の実施形態のファイル内容読み出しとの主な違いは、暗号ファイル 4 3 の内容データ 4 1 1 の読み出しにおいて、内容データ 4 1 1 は復号化されずそのまま読み出される点である。

【0063】図 3 は、図 1 から携帯記録装置 5、復号ルーチン 3 4、および復号鍵取得ルーチン 3 3 を除いた図であり、プロセス 1 が平文ファイル 4 2 または暗号ファイル 4 3 に対しコピー読み出しをする動作を示している。平文ファイル 4 2 に関しては、第 1 の実施形態と同じであるから説明は省略する。

【0064】暗号ファイル 4 3 に関しては、第 2 の実施形態の場合、第 1 の実施形態と異なり、内容データ 4 1 1 は復号化されず、そのままプロセス 1 に渡される。つまり、暗号ファイル 4 3 は平文ファイル 4 2 と同様に扱われる。

【0065】本発明の第 3 の実施形態のプロセス管理について図 4 を参照して説明する。図 5 は、プロセス 1、保護プロセス 6、OS 2、FS 3、記録装置 4 およびユーザインタフェース装置 7 から構成されるコンピュータシステムの図である。保護プロセス 6 は、暗号ファイル 4 3 に対し、第 1 の実施形態で説明した内容読み出しを行い、その内容データ 4 1 1 の復号結果を取得したプロセス 1 である。つまり、プロセス 1 が暗号ファイル 4 3 の内容読み出しに成功すると、そのプロセス 1 は保護プロセス 6 となる。ユーザインタフェース装置 7 は、ユーザへの一時的な情報提供のためのインタフェースに供される出力装置であり、例えば、ディスプレイやスピーカである。

【0066】第 3 の実施形態では保護プロセス 6 に対する出力制限に関する実施形態を示す。プロセス 1 あるいは保護プロセス 6 からの出力は必ず OS 2 を通じて行われることを利用し、この制限は具体的には OS 2 によって行われる。OS 2 は、FS 3 から読み出し結果を取得する際に暗号ファイル 4 3 の読み出し結果であることを通知され、このデータを渡すプロセス 1 を保護プロセス 6 であるとする。

【0067】プロセス 1 に関しては、保護プロセス 6 を

含む他のプロセス1、記録装置4およびユーザインタフェース装置7への情報出力は何れも可能であり、他のプロセス1および記録装置4からの情報入力は何れも可能である。

【0068】保護プロセス6に関しては、ユーザインタフェース装置7への情報出力は可能であるが、保護プロセス6を含む他のプロセス1および記録装置4への情報出力は、OS2による制限により不可能である。一方、他のプロセス1および記録装置4からの情報入力が可能である。

【0069】次に、本発明の第4の実施形態のファイル書き込みについて説明する。この実施形態では、図5に示すように、プロセス1によりファイル41の書き込みを行う。すなわち、プロセス1は、OS2、FS3を通じ、記録装置4に対し、任意のファイル名に対応付けられたファイル4を作成できる。

【0070】次に、本発明の第5の実施形態の識別子および復号鍵の登録について図6を参照して説明する。図6では、復号鍵51および識別子413を識別子・復号鍵管理データベース8に登録する様子を示している。この作業は、ユーザ間で流通される暗号ファイル43に対してユーザが利用を希望する場合に、利用するために必要な復号鍵51をそのユーザに対して供給することを可能とするために、暗号ファイル43の著作者によって行われる。

【0071】暗号ファイル43の著作者は、その暗号ファイル43の内容データ411を暗号属性412に示される復号アルゴリズムで復号するときに必要な復号鍵51と、その暗号ファイル43の識別子413を組にして、識別子・復号鍵管理データベース8に登録する。

【0072】次に、本発明の第6の実施形態の復号鍵の購入について図7を参照して説明する。図7は識別子・復号鍵管理データベース8から復号鍵51と識別子413の組をもらい、携帯記録装置5へ格納する様子を示している。この作業は、暗号ファイル43の利用を希望するユーザが、自分の持つ携帯記録装置5へ利用するために必要な復号鍵51を格納するため、ユーザによって行われる。著作権を保護することの中の重要な要素に利用するユーザから確実に対価を徴収することがあるが、図7に示される作業は暗号ファイル43の利用権をユーザに与える作業であるといえ、この作業をユーザが行う際にユーザに何らかの方法で課金を強制することで、上記目的を達成することができる。

【0073】ユーザは利用を希望する暗号ファイル43の識別子413に対応する復号鍵51を識別子・復号鍵管理データベース8へ要求し、識別子・復号鍵管理データベース8はユーザの携帯記録装置5へ復号鍵51を格納し、同時に、格納した復号鍵51を対応する識別子413を使って後から検索できるような情報を復号鍵管理情報52として記録する。

【0074】次に、本発明の第7の実施形態のリンクファイル内容読み出しについて図8および図9を参照して説明する。図8はリンク属性414を複数個持つファイル41を示しており、図9はリンク属性414を構成する項目を示している。以下、リンク属性414を少なくとも1つ持つファイル41をリンク元ファイルという。以下ではリンク元ファイルに対して内容読み出しサービスを要求された場合のFS3の動作を説明する。

【0075】FS3は対象となっているリンク元ファイルの内容データ411を取得する。このリンク元ファイルにはいくつかのリンク属性414が含まれているが、FS3はこれらすべてのリンク属性414のそれぞれに対し以下の操作を行う。

【0076】まず、FS3は、リンク属性414のリンク先ファイル名4141を調べ、これに示されるファイル41の読み出しを試みる。ここではとりあえずこのファイル41はリンク属性414を持たないとする。このファイル41はこれまでに説明した方法で読み出すことが可能であり、FS3は読み出し結果のデータを取得する。次にFS3は、リンク属性414の挿入部位4143を調べ、これに示される部分を、取得したデータから抽出する。挿入部位4143は、例えば47バイト目から73バイト目といった意味を持つ可変長の値である。

【0077】更にFS3は、リンク属性414の挿入位置4142を調べ、リンク元ファイルの内容データ411中の、この挿入位置4142に示される位置に、抽出したデータを挿入する。挿入位置4142の示す値に関しては、例えば、リンク属性414によってデータが挿入された後の位置を示すのではなく、あくまでリンク元ファイルの内容データ411中の位置を示すとすれば、リンク属性414を処理する順番に関わらず、一定の挿入結果が得られる。あるいは、データが挿入された後の位置を示すとしても、リンク属性414を処理する順番を一定にすれば、一定の挿入結果が得られる。

【0078】上記操作において、例えばファイル41が存在しない等の理由で、リンク先ファイル名4141に示されるファイル41の読み出しに失敗することがある。この場合、FS3は、ファイル41の読み出し結果を挿入する代わりに、読み出しエラー対処4144に示される処理を実行する。この処理には、例えば、各バイトの値が0である指定サイズのデータの挿入であったり、指定サイズの指定データの挿入であったり、あるいは何も挿入しない、といった動作があり得る。

【0079】このようにして、リンク元ファイルの持つすべてのリンク属性414について上記の操作が終了したなら、FS3はこれらの操作によって元のサイズより増大したであろうリンク元ファイルの内容データ411を要求元に渡す。

【0080】上記の操作において、リンク先ファイル名4141の示すファイル41はリンク属性414を持た

ないファイル 4 1 であると仮定した。以下ではリンク先ファイル名 4 1 4 1 の示すファイル 4 1 がリンク属性 4 1 4 を持つ場合を説明する。この場合、F S 3 はリンク先ファイル名 4 1 4 1 に示されるファイル 4 1 の内容の読み出しを行い、次にこのファイル 4 1 の持つすべてのリンク属性 4 1 4 に対し、上記と同じ操作を行う。つまり、リンク先ファイル名 4 1 4 1 が示すファイル 4 1 がさらにリンク属性 4 1 4 を持つ場合は、上記の操作を再帰的に行うことになる。その他は上記と同様である。

【0081】次に、本発明の第 8 の実施形態のリンクファイル非展開内容読み出しについて説明する。F S 3 は内容読み出しのモードとして非展開モードを提供し、リンク属性 4 1 4 は図 9 に示すようにリンク先ファイル名 4 1 4 1、挿入位置 4 1 4 2、挿入部位 4 1 4 3、読み出しエラー対処 4 1 4 4 に加えて非展開対処 4 1 4 5 なる項目を持つ。非展開対処 4 1 4 5 の記述形式は読み出しエラー対処 4 1 4 4 と同様のものであり、例えば、各バイトの値が 0 である指定サイズのデータの挿入であったり、指定サイズの指定データの挿入であったり、あるいは何も挿入しないといった動作を示す可変長の値として記述される。

【0082】F S 3 は、少なくとも 1 つのリンク属性 4 1 4 を持つリンク元ファイルを対象とした非展開モードの内容読み出しを要求された場合、まず F S 3 は対象となっているリンク元ファイルの内容データ 4 1 1 を取得し、更にリンク元ファイルが含むすべてのリンク属性 4 1 4 のそれぞれに対し非展開対処 4 1 4 5 に示される動作を行う。この処理はリンク先ファイル名 4 1 4 1 に示されるファイル 4 の有無に関係なく行われる。この動作がすべてのリンク属性 4 1 4 についてなされた後、F S 3 はこれらの操作によって元のサイズより増大したであろうリンク元ファイルの内容データ 4 1 1 を要求元に渡す。

【0083】次に、本発明の第 9 の実施形態のリンク暗号ファイル内容読み出しについて説明する。ファイル 4 1 が属性として暗号属性 4 1 2 とリンク属性 4 1 4 を同時に持つ場合の内容読み出しの動作について説明する。この場合、F S 3 の基本的な動作は第 7 の実施形態と同様であるが、内容読み出しの対象となるファイル 4 1 の暗号属性 4 1 2 に何らかの暗号アルゴリズムが設定されているときに、読み出したデータを第 1 の実施形態のように復号化するという点で第 7 の実施形態と異なる。つまり、リンク元ファイルの暗号属性 4 1 2 に何らかの暗号アルゴリズムが設定されているときは、リンク元ファイルの内容データ 4 1 1 を第 1 の実施形態のように復号化した後に、リンク元ファイルのすべてのリンク属性 4 1 4 それぞれに対する処理を第 7 の実施形態のように行う。

【0084】次に、本発明の第 10 の実施形態のプロセス管理について説明する。上述した第 3 の実施形態で

は、暗号ファイル 4 3 に対して内容読み出しを行い、その内容データ 4 1 1 の復号結果を取得したプロセス 1 を保護プロセス 6 とし、O S 2 は保護プロセス 6 に対する出力制限を行ったが、第 10 の実施形態では、暗号属性 4 1 2 とリンク属性 4 1 4 を同時に持つファイル 4 1 に対する内容読み出しを行った場合の O S 2 のプロセス 1 に対する出力制限を説明する。

【0085】O S 2 が F S 3 に対して、リンク属性 4 1 4 を持つファイル 4 1 を対象とした内容読み出しサービスを要求したとき、F S 3 は第 9 の実施形態のように複数のファイル 4 1 を読み出す。この一連の読み出しの対象となったファイル 4 1 のうち、少なくとも 1 つのファイル 4 1 の暗号属性 4 1 2 に何らかの暗号アルゴリズムが設定されているとき、F S 3 は、読み出し結果を O S 2 に渡すとき、O S 2 は暗号ファイル 4 3 の読み出し結果であることを通知する。O S 2 はこのデータを渡すプロセス 1 を保護プロセス 6 であるとし、第 3 の実施形態と同様の出力制限を保護プロセス 6 に課す。

【0086】

【発明の効果】以上説明したように、本発明によれば、デジタルデータを自由に流通しつつも正当な利用者のみが利用可能であり、テキストデータのような汎用的なフォーマットのファイルであっても、これを再利用する場合に元の作者の著作権を保護することができ、ユーザは一度利用権を取得すると、コンピュータを問わずに利用することができる。すなわち、デジタルデータの低コストなコピーや転送が容易という特徴を生かしつつ、汎用的に扱えるデジタルデータの不正利用を防止し、作者の著作権を保護することができ、デジタルデータの作成に関与したすべての作成者に対して著作権を保護することができ、デジタルデータに対する利用権をコンピュータ毎でなくユーザ毎に付与することができる。

【図面の簡単な説明】

【図 1】本発明の第 1 の実施形態に係る著作権保護システムの構成を示すブロック図である。

【図 2】図 1 の著作権保護システムに使用されるファイルの構成を示す図である。

【図 3】本発明の第 2 の実施形態に係るファイルコピー読み出し動作を説明するための著作権保護システムの構成を示す図である。

【図 4】本発明の第 3 の実施形態に係るオペレーティングシステムがプロセスに対して行う出力制限であるプロセス管理を説明するための著作権保護システムの構成を示す図である。

【図 5】本発明の第 4 の実施形態に係るファイル書き込み動作を説明するための著作権保護システムの構成を示す図である。

【図 6】本発明の第 5 の実施形態において作者による復号鍵と識別子の組を識別子・復号鍵管理データベースへ登録する動作を説明するための図である。

【図 7】本発明の第 6 の実施形態における復号鍵の購入を説明するための図である。

【図 8】本発明の第 7 の実施形態におけるリンクファイル内容読み出しに使用されるリンク属性を有するファイルの構成を示す図である。

【図 9】リンク属性の構成を説明するための図である。

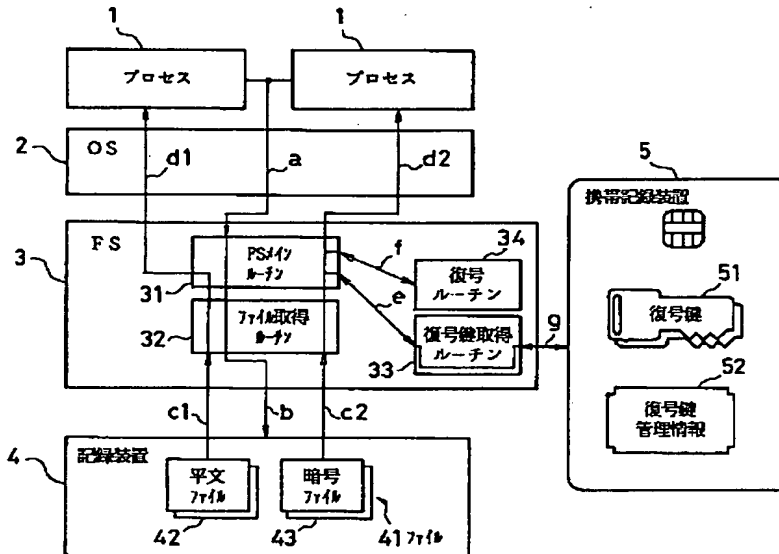
【図 10】従来のファイル読み出し手順を説明するためのコンピュータシステムの構成を示す図である。

【符号の説明】

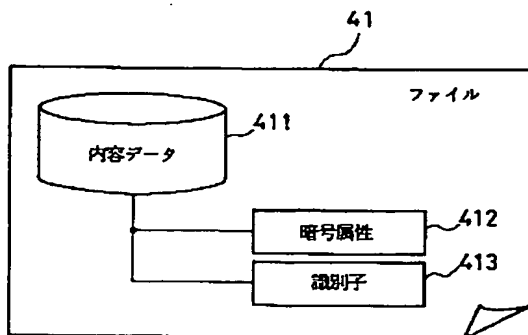
- 1 プロセス
- 2 オペレーティングシステム (OS)
- 3 ファイルシステム (FS)
- 4 記録装置

- 5 携帯記録装置
- 6 保護プロセス
- 7 ユーザインタフェース装置
- 8 識別子・復号鍵管理データベース
- 31 FSメインルーチン
- 32 ファイル取得ルーチン
- 33 復号鍵取得ルーチン
- 34 復号ルーチン
- 41 ファイル
- 42 平文ファイル
- 43 暗号ファイル
- 51 復号鍵
- 52 復号鍵管理情報

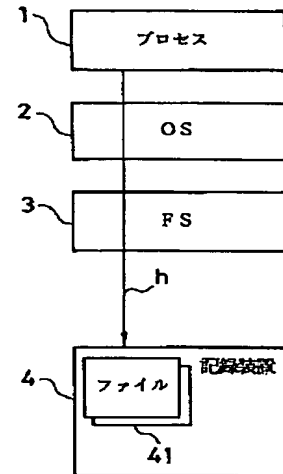
【図 1】



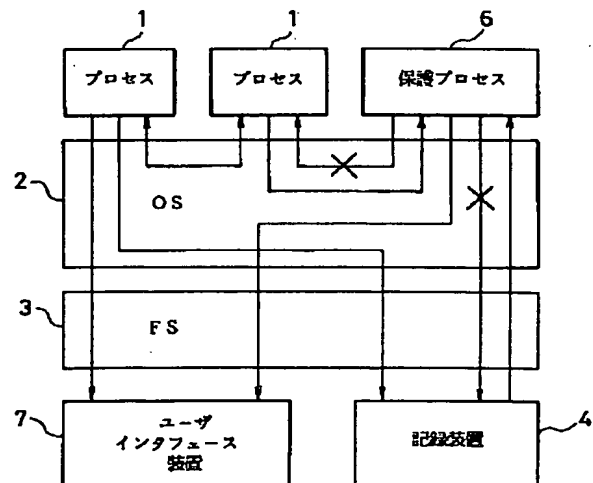
【図 2】



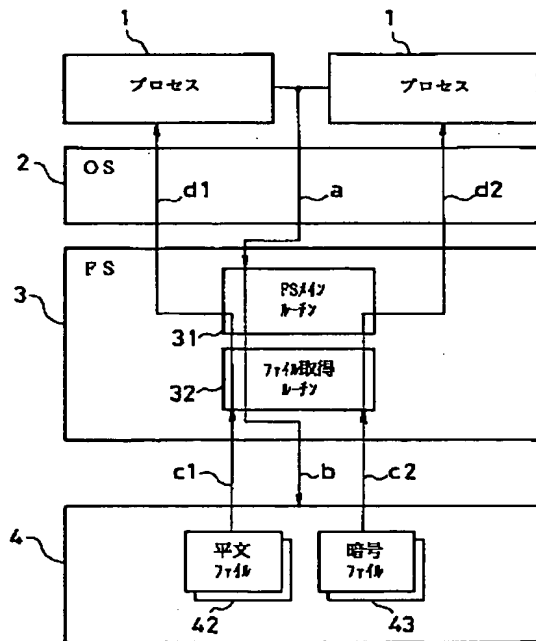
【図 5】



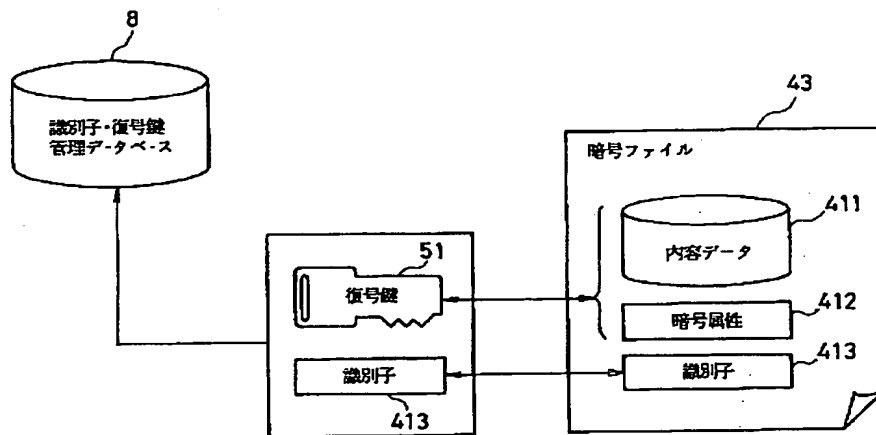
【図 4】



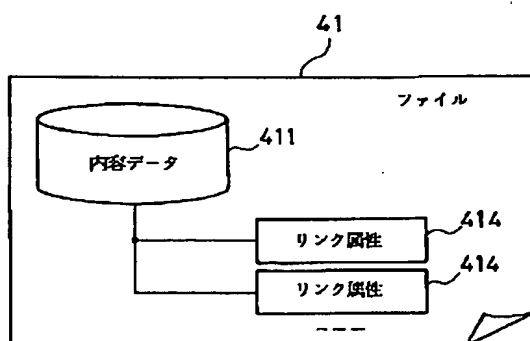
【図 3】



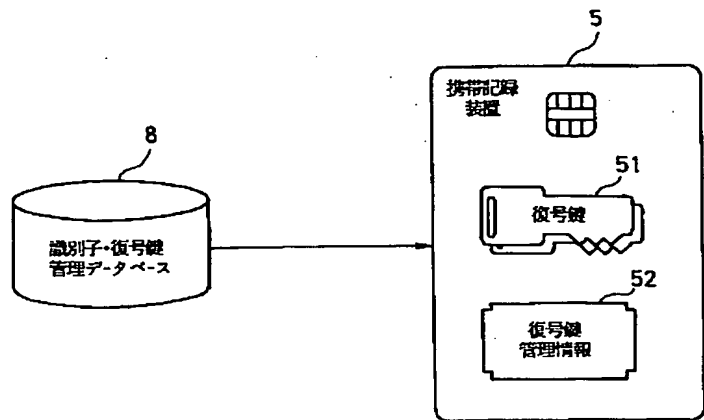
【図 6】



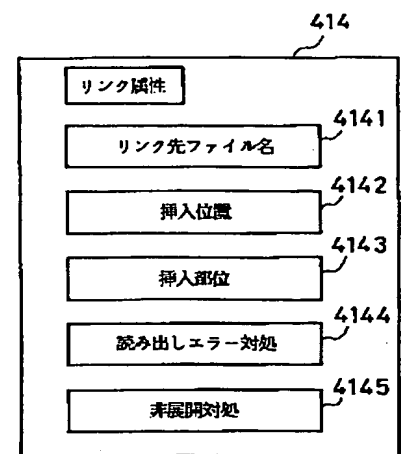
【図 8】



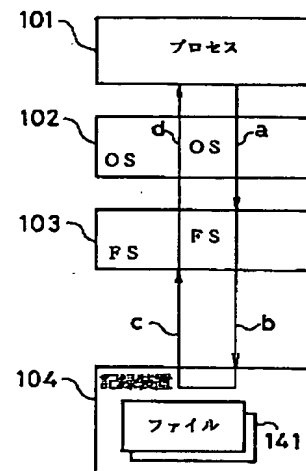
【図 7】



【図 9】



【図 10】



フロントページの続き

(51) Int. Cl. ⁶

識別記号

G 0 9 C 1/00

6 6 0

H 0 4 L 9/08

F I

G 0 6 F 15/20

Z

H 0 4 L 9/00

6 0 1 B